Office of the Governor
State Chief Information Officer

SECURITY

Chapter 2 – Controlling Access to Information and Systems

Scope: These standards apply to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services."

.

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Controlling Access to Information and Systems

020101 Managing Access Control Standards

Purpose: To establish requirements for controlling access to State information assets.

STANDARD

Access to State information technology assets shall be controlled and managed to ensure that only authorized devices/persons have access as is appropriate for an agency in accordance with the agency's business needs.

All computers that are permanently or intermittently connected to internal computer networks shall have an approved password-based access control system. Regardless of the network connections, all computers handling confidential information shall employ approved password-based access control systems. Only authorized users shall be granted access to the State's information systems, and the principle of least privilege shall be used and enforced. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.

Access shall be controlled by the following:

- Standard user profiles (see ISO 17799 §11.1.1.1f).
- Documented semi-annual review of users' rights (see ISO 17799 §11.2.4a).
- Documented review of privileged accounts every quarter (see ISO 17799 §11.2.4b).
- Restriction of connection time (see ISO 17799 §11.5f).
- Immediate termination of access upon severance or leaving employment

To ensure that data processed are the actual data required by the data custodian, predetermined times for processing those data must be set by the interested parties to protect the integrity of the data (e.g., preset batch file transmission times) (see ISO 17799 §11.5.6).

ISO 17799: 2005 REFERENCES
11.1.1 Access control policy
11.2.4 Review of user access rights
11.5.6 Limitation of connection time

020102 Managing User Access

Purpose: To prevent unauthorized access to agency networks.

STANDARD

Agencies shall be responsible for establishing a procedure for managing access rights for users of their networks throughout the life cycle of the user ID.

Only authorized users shall be granted access to State information systems. Users shall be responsible for maintaining the security of their user IDs and passwords. User IDs shall be individually assigned in order to maintain accountability. Each user ID shall be used by only a single individual, who is responsible for every action initiated by the account linked to that user ID. Where supported, the system shall display (after successful login) the date and time of last use of the individual's account so that unauthorized use may be detected.

Logging of Administrator Activity

All user ID creation, deletion and change activity performed by system administrators and others with privileged user IDs shall be securely logged and reviewed on a regular basis.

Concurrent Connections

For those systems that enforce a maximum number of concurrent connections for an individual user ID, the number of concurrent connections must be set to two (2).

Outside User IDs

User IDs established for a nonemployee/contractor must have a specified expiration date unless the provision of a user ID without a specified expiration date is approved in writing by the agency security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.

Access control may need to be modified in response to the confidentiality of information contained on the system, if existing access controls pose a risk that confidentiality may be breached.

ISO 17799: 2005 REFERENCE
11.2 User access management

020103 Securing Unattended Work Stations

Purpose: To prevent unauthorized system access.

STANDARD

Workstations shall be safeguarded from unauthorized access—especially when left unattended. Each agency shall be responsible for configuring all workstations to require a password-protected screen saver after a maximum of thirty (30)

minutes of inactivity. Users shall not disable the password-protected configuration specifications established by their agency.

ISO 17799: 2005 REFERENCES
11.3.2 Unattended user equipment
11.3.3 Clear desk and clear screen policy

020104 Managing Network Access Controls

Purpose: To establish requirements for the access and use of the State Network and agency networks.

STANDARD

Access to networks operated by State agencies, including the State Network, shall be controlled to prevent unauthorized access and to prevent malicious attacks on the networks. Access to all agency computing and information systems shall be restricted unless explicitly authorized.

- All remote access (dial-in services) to the networks shall be either through an approved modem pool or via an Internet service provider (ISP).
- Remote users shall connect to the State Network only using protocols approved by the State Chief Information Officer (State CIO). Remote users with direct connections to agency networks shall follow agency protocols.
- When users on the agency networks connect to external systems, including the State Network, they shall comply with the State CIO's Use of the State Network and the Internet Standard.
- Users on the State Network shall not be connected to the State Network at the same time as they are using a modem to connect to an external network.
- Users shall not extend or retransmit network services in any way without appropriate management approval.
- Users shall not install network hardware or software that provides network services, such as routers, switches, hubs and wireless access points, without appropriate management approval.
- Non–State of North Carolina computer systems that require connectivity to the State Network shall conform to statewide security standards.
- Non–State of North Carolina computer systems that require connectivity to agency networks shall conform to agency security standards.
- Users shall not download, install or run security programs or utilities that reveal weaknesses in the State Network without prior written approval from the State CIO. Users shall not download, install or run security programs or utilities that reveal weaknesses of agency networks without appropriate agency management approval. For example, State users must not run password-cracking programs, packet sniffers, network-mapping tools or port scanners while connected in any manner to the State Network infrastructure. Users shall not be permitted to alter network hardware in any way.

ISO 17799: 2005 REFERENCE
11.4 Network access control

020105 Controlling Access to Operating System Software

Purpose: To limit access to operating system software to those individuals authorized to perform system administration/management functions.

STANDARD

Only those individuals designated as system administrators shall have access to operating system commands. System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application ports are opened in the system's firewall.

- Internal network addresses and configuration and other system design information shall be limited to only those individuals who require access in the performance of tasks or services essential to the fulfilment of a work assignment, contract or program.
- State agencies shall maintain a list of administrative contacts for their systems.
- All authorized users of administrative-access accounts shall have management instructions, documentation and training.
- Each individual who uses an administrative-access account shall use the account only for administrative duties. For other work being performed, the individual shall use a regular user account.
- Each account used for administrative access shall comply with Standard 020106, Managing Passwords.
- When special-access accounts are needed for internal or external audit, software development, software installation, or other defined need, they shall be authorized in advance by management and shall be:
    - ❑ Created with a specific expiration date.
    - ❑ Removed when the work is completed.
- Administrative-access accounts must connect in a secure manner at all times.

ISO 17799: 2005 REFERENCE
11.5 Operating System Access Control

020106 Managing Passwords

Purpose: To prevent unauthorized access and to establish user accountability when using IDs and passwords to access State information systems.

STANDARD

Agencies shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access State information systems. The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are selected as the method of performing identification and

authentication. A unique user ID shall be assigned to each user so that individual accountability can be established for all system activities. Management approval shall be required for each user ID created. A process shall be in place to remove, suspend or reassign user IDs that become inactive as a result of employee or contractor movements. The system's authentication system shall limit unsuccessful logon attempts. Information shall be maintained on all logon attempts to facilitate intrusion detection. Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long-life passwords. Each agency shall evaluate its business needs and the associated risks for its information systems in conjunction with identification and authentication requirements. When IDs and passwords are selected as the method of performing identification and authentication, agencies are required to select and use the appropriate standards and best practices. Agencies must specify the minimum requirements for identification and authentication using IDs and passwords in accordance with the standard criteria that follow. Depending on the operating environment and associated exposures, additional or more stringent security practices may be required.

- For secured access to systems and applications that require a low level of security, passwords shall have at least six (6) characters of any sort.
- For access to all systems and applications that require a high level of security, such as electronic fund transfers, taxes and credit card transactions, passwords shall be at least eight (8) characters.
- To the extent possible, passwords shall be composed of a variety of letters, numbers and symbols[1] with no spaces in between.
- To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
- Passwords shall not contain dictionary words or abbreviations.
- Passwords shall not contain number or character substitutes to create dictionary words (e.g., *d33psl33p* for *deep sleep*[2]).
- Passwords for internal State resources shall be different from passwords for external, non-State resources.
- Password generators that create random passwords shall be allowed.
- Password management application features that allow users to maintain password lists and/or automate password inputs shall be prohibited, except for simplified/single sign-on systems approved by the State Chief Information Officer (State CIO).

Password Management Standards

- Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.

---

[1] For Resource Access Control Facility (RACF), valid symbols are @, $, #, and _, and the first character of a password must be a letter and the password must contain a number.

[2] Other examples of numbers/symbols for letters are *0* for *o*, *$* or *5* for *S*, *1* for *i*, and *1* for *l*, as in *capta1n k1rk* or *mr5pock*.

- Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the State CIO.
- No automated password input shall be allowed, except for simplified/single sign-on systems that have been approved by the State CIO.
- Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. If stored, Passwords shall be stored in encrypted format.
- Individual user passwords (e.g., email, Web and calendar) used to access systems and applications shall be changed at least every ninety (90) days. Passwords shall not be reused until six additional passwords have been created.
- Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.
- Where possible and practicable, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law, if the inactivity period is shorter than thirty (30) minutes.
- Passwords shall not be displayed in clear text during the logon process or other processes. Where possible, applications that require clear-text authentication shall be converted to equivalents that can use encryption.[3]
- Passwords shall be changed whenever there is a chance that the password or the system could be compromised.

Password Management Standards—System Administrators

- All passwords (e.g., Unix, NT and RACF) shall be changed at least every ninety (90) days. Passwords for administrative user accounts and accounts with special privileges shall be changed at least every thirty (30) days.
- A user account that has system-level privileges or programs such as root access shall have a different password from all other accounts held by that user.
- Password files shall be retrievable only by the security administrator or a designated backup security administrator.
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed.
- The password for a shared administrative-access account shall change when any individual who knows the password leaves the agency that established the account or when job responsibilities change.
    - In situations where a system has only one administrator, agencies shall establish a password escrow procedure so that, in the absence of the administrator, someone can gain access to the administrator account.

[3] Encryption is defined in the Security Architecture Chapter, Standard 3, Use Cryptography Based on Open Standards.

ISO 17799: 2005 REFERENCES
11.2.3 User password management
11.3.1 Password use
11.5.1 Secure log-on procedures
11.5.2 User identification and authentication
11.5.3 Password management system

020107 Securing Against Unauthorized Physical Access

Purpose: To protect the State's information technology assets with appropriate physical controls.

STANDARD

Physical access to areas housing information technology assets is to be appropriately controlled. Authorized individuals may include State employees, contractors and vendors. Agencies shall develop access policies for authorized individuals as well as visitors to these areas. An audit trail of access for all individuals shall be maintained.

ISO 17799: 2005 REFERENCE
9.1.2 Physical entry controls

020108 Restricting Access

Purpose: To ensure that information system access is granted only to authorized users.

STANDARD

Agencies shall establish appropriate controls on access to information systems to allow only those authorized to access the data residing on those systems to do so.

Users of agency information systems shall be provided access to information and system functions in accordance with Standard 020101, Managing Access Control Standards.

Access to confidential information shall be restricted to authorized individuals who require access to the information as part of their job responsibilities.

An agency may change, restrict or eliminate user access privileges at any time.

ISO 17799: 2005 REFERENCE
11.6.1 Information access restriction

020109 Monitoring System Access and Use

Purpose: To establish requirements and guidelines for policies that disclose to employees and third-party contractors using State information systems the situations in which and the purposes for which filtering and monitoring may occur.

STANDARD

Agencies shall have the right and ability to monitor and filter use of information systems by employee and third-party contractor users.

State agencies using monitoring and filtering technologies must establish policies to provide adequate notice to State employees and third-party contractors of what the agency will be filtering and/or monitoring. The policies shall include the circumstances under which filtering and monitoring will take place. The policies shall also state that users shall have no expectation of privacy unless expressly granted by an agency.

Agencies using filtering and monitoring must:

- Examine the relevant information technology processes and determine all instances in which individually identifiable information is collected when an employee or third-party contractor uses agency information resources.
- Specify in their written policies the scope and manner of monitoring for any information system and never exceed the scope of any written monitoring statement in the absence of any clearly stated exception.
- Obtain a written receipt from State employees and third-party contractors acknowledging that they have received, read and understood the agency's filtering and monitoring policies.
- Inform State employees and third-party contractors of any activities that are prohibited when using the agency's information systems.

ISO 17799: 2005 REFERENCE
10.10.2 Monitoring system use

020110 Giving Access to Files and Documents

Purpose: To prevent the unauthorized or accidental copying, moving, editing or deleting of data and to protect the confidentiality, integrity and availability of the information assets of North Carolina.

STANDARD

Custodians of data shall assign staff the responsibility for administering and maintaining the rights and permissions for accessing the data and information.

- Users shall be provided with access to information and systems in accordance with a defined standard of access control such as:
    - ❑ Discretionary access control.
    - ❑ Mandatory access control.
    - ❑ Lattice-based access control.
    - ❑ Rule-based access control.
    - ❑ Role-based access control.
    - ❑ Access control lists.
- The default for access is role-based access control for files and documents.

- Access rights of users in the form of read, write and execute shall be controlled appropriately and the outputs of those rights shall be seen only by authorized individuals.
- User rights shall be reviewed at six (6)-month intervals.
- A three (3)-month review cycle shall be required for special access privileges. General user access rights shall be reviewed regularly to ensure that unauthorized privileges have not been obtained.

ISO 17799: 2005 REFERENCE
11.2.4 Review of user access rights

020111 Managing Higher Risk System Access

Purpose: To protect the confidentiality, integrity and availability of data on high-risk information technology systems in State government.

STANDARD

Certain systems and applications, because of the nature of the data contained in them, require special management oversight and shall be classified as high-risk. Many times these high-risk systems contain confidential data. At a minimum, these systems shall require access control equal to that specified in Standard 020101, Managing Access Control Standards.

All systems and applications shall be classified through a risk assessment to determine, in part, whether they are high-risk systems.

GUIDANCE

At a minimum, the following should be considered when implementing controls for high-risk systems:

- Whether access to the system is allowed from an external site.
- Hardening of the operating system.
- Criminal Background checks of personnel, vendors and contractors in contact with the system and applications.
- Disaster recovery planning.
- The consequences of loss of data security.

ISO 17799: 2005 REFERENCE
11.6.2 Sensitive system isolation

020112 Controlling Remote User Access

Purpose: To require users of State information technology systems who access agency information technology systems remotely to do so in a secure manner.

STANDARD

Authorized users of agency computer systems, the State Network and data repositories shall be permitted to remotely connect to those systems, networks and data repositories for the conduct of State-related business only through secure, authenticated and carefully managed access methods.

Access to the State Network and agency internal networks via external connections from local or remote locations including homes, hotel rooms, wireless devices and off-site offices shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit request is made by the user and approved by the manager for the system in question.

Opening uncontrolled or unsecured paths into any element of the State Network that requires security or to internal computer systems presents unacceptable risk to the entire State infrastructure.

Statewide Standard for Remote Access

Access shall be permitted through an agency-managed secure tunnel such as a Virtual Private Network (VPN) or other open standard protocol such as Secure Shell (SSH) or Internet Protocol Security (IPSec) that provides encryption and secure authentication.

Authentication

- The authentication and authorization system for remote access shall be managed by the agency. Agencies that need centralized network infrastructure services, such as Public Key Infrastructure (PKI), shall use the state-wide authentication and authorization service known as NCID .
- Authentication for remote access shall be strong. Passwords shall not traverse the network in clear text and must meet minimum requirements as documented in approved security policies and standards. Each user who remotely accesses an internal network or system shall be uniquely identifiable.

Users

- User IDs: All users who require remote access privileges shall be responsible for the activity performed with their user IDs. User IDs shall never be shared with those not authorized to use the ID. User IDs shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user IDs belonging to others.
- Revocation/modification: Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon an employee’s or contractor’s termination from service. Remote access privileges shall be reviewed upon an employee’s or contractor’s change of assignments and in conjunction with regularly scheduled security assessments.
- Anonymous interaction: With the exception of Web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any ITS system or network anonymously (for example, by using “guest” user IDs). If users employ system facilities that allow them to change the active user ID to gain certain privileges, they must have initially logged in employing a user ID that clearly indicates their identity.

Configuration

- Default to denial: If an agency computer or network access control system is not functioning properly, it shall default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.
- Privilege access controls: All computers permanently or intermittently connected to external networks must operate with privilege access controls approved by the agency. Multi-user systems must employ user IDs unique to each user, as well as user privilege restriction mechanisms, including directory and file access permissions.
- Antivirus and firewall protection: External computers or networks making remote connection to internal agency computers or networks shall utilize an agency-approved active virus scanning and repair program and an agency-approved personal firewall system (hardware or software). The agency shall ensure that updates to virus scanning software and firewall systems are available to users. External computers or networks making a remote connection to a public Web server are exempted.
- Time-out: Network-connected single-user systems shall employ agency-approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity (for example, a screen saver). To the extent possible, all systems accepting remote connections from public-network-connected users (users connected through dial-up phone modems, dial-up Internet service providers, or broadband, i.e., DSL or cable modems) shall include a time-out system. This time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the State Network. In addition, all user IDs registered to networks or computers with external access facilities shall be automatically suspended after a period of thirty (30) days of inactivity.
- Failure to authenticate: To the extent possible, all systems accepting remote connections from public-network-connected users shall temporarily terminate the connection or time out the user ID following a sequence of several unsuccessful attempts to log in. For example, if an incorrect dynamic password is provided three consecutive times, dial-up systems shall drop the connection. Repeated unsuccessful attempts to remotely establish a connection using a privileged user ID shall not result in the revocation (suspension as opposed to time-out) of the user ID because this could interfere with the ability of authorized parties to respond to security incidents.
- Modems on desktop/laptop systems: Management must approve the use of modems and the communications software used with modems. Existing modems connected to a LAN that are used for remote control and file transfer from a remote location to LAN desktops must be replaced as soon as possible with a secure TCP/IP or VPN connection. Unless a dynamic password system is installed, workers with home-based, mobile or telecommuting PCs shall not leave modems in auto-answer mode, with communications software enabled, such that incoming dial-up calls could be received.
- VPN and/or other secure communication protocols shall be used to communicate with agency business systems.

- For client-to-server/gateway VPN solutions, split tunnelling shall not be permitted (via configuration option).

Access to Single-Host Systems

- Remote access to single-equipment hosts (i.e., agency servers, Web-hosting equipment) shall be permitted provided that these requirements are met:
    - Dial-up modem service: An agency shall provide dial-up modem service *only if* that service is limited exclusively to agency employees and contractors.
    - Web-hosting servers shall provide anonymous or authenticated access to pages *only if* the service host prevents onward connection to the State Network.
- Management consoles and other special needs: Users requiring modem access for "out of band" management or special needs must obtain agency security administrator approval for the modem and its use as set forth in agency procedures. Each agency shall establish procedures to approve modems on an individual basis. Any dialup server that grants network access must authenticate each user, minimally, by a unique identification with password and shall encrypt the data stream. All calls must be logged, and logs of access shall be retained for ninety (90) days. At the completion of each dial-up session to a server, the accessing workstation shall be secured via password.

Miscellaneous

- Disclosure of systems information: The internal addresses, configurations and related system design information for agency computers and networks shall be kept confidential and shall not be released to third parties who do not have a demonstrable need to know such information. Likewise, the security measures employed to protect agency computers and networks shall be kept confidential and shall be similarly protected.
- Systems shall support the capability for all remote access occurrences to be logged (user ID, date/time, and duration of connection at a minimum).
- There shall be certain remote-access users who warrant use of file/disk encryption technology. This is based on whether confidential records are included in the information that they are able to store on their local systems.
- Audit: Audit logs of remote-access activities shall be maintained for at least ninety (90) days.

Related information
Standard 050404 Working from Home or Other Off-Site Location

ISO 17799: 2005 REFERENCE
11.4.2 User authentication for external connections

020113 Types of Access Granted to Third Parties

Purpose: To establish access standards for third parties.

STANDARD

Third party access to State and/or Agency resources shall be controlled using physical and logical safeguards.

RELATED INFORMATION

020101 Managing Access Control Standards

020102 Managing User Access

020108 Restricting Access

020110 Giving Access to Files and Documents

ISO 17799: 2005 REFERENCE
6.2.1 Identification of risks related to external parties

020114 Why Access is Granted to Third Parties

Purpose: To establish access standards for third parties.

STANDARD

Third party access to State and/or Agency resources shall be granted on a need to have basis.

RELATED INFORMATION

020101 Managing Access Control Standards

020102 Managing User Access

020108 Restricting Access

020110 Giving Access to Files and Documents

ISO 17799: 2005 REFERENCE
6.2.1 Identification of risks related to third parties

020115 Access Control Framework

Purpose: To establish standards for Agencies accessing the State network.

STANDARD

Agencies shall follow the attached matrix, Security Framework Template, to prevent unauthorized access to information systems through appropriate placement and configuration that provides protective measures that are commensurate with the security level required to protect the data contained in those systems.

Agencies shall assess the risk associated with each business system to determine what security rules apply to the system and/or application. The security assessment determines the appropriate placement of each system and application within the security framework and evaluates the network resources, systems, data and applications based upon their criticality. The assessment assigns correlative security requirements. As the critical nature of the data and

applications increases, the security measures required to protect the data and applications also increase.

Security Requirements
Security for the network infrastructure and for distributed systems operated by state agencies shall comply with the security requirements of the template, which is attached and is expressly made part of this policy. All executive branch agencies capable of meeting the security requirements for the Demilitarized Zone (DMZ) and/or Secure Zone as listed in the template shall do so.

Special Assembly Security Requirements
Agencies not able to adhere to the DMZ and/or security requirements shall develop a Special Assembly zone and document the rationale for developing the Special Assembly zone. Security controls in the Special Assembly area are not as structured as controls in the DMZ/Secure zones. Agencies acknowledge that additional security risks are associated with the Special Assembly zone.

Office of the Governor
State Chief Information Officer

Security Framework Template

	DMZ			Secure Zone				Special Assemblies				
Destination ->	**User Facing**			**Application Serv.**		**DB Services**		**Mgmt.**	**Application Unique**	**Agency**	**Infrastructure State WAN**	
	Public	**State**	**Vendor**	**Std.**	**High**	**Std.**	**High**	**Domain**	**Domain*******	**Internal LAN**	**Std.**	**High**
Operational Controls												
User/Device												
Access	Yes	Yes	Yes	Opt.	No	No	No	No	Yes	Yes	Yes	Yes
Authentication*	Opt.	Opt.	Opt.	Req.	N/A	N/A	N/A	N/A	TBD	Opt.	Opt.	Req.
Authorization	Opt.	Opt.	Opt.	Req.	N/A	N/A	N/A	N/A	TBD	Opt.	Opt.	Req.
Encryption**	Opt.	Opt.	Opt.	Opt.	N/A	N/A	N/A	N/A	TBD	Opt.	Opt.	Opt.
Administrator												
Access	Yes	Yes	Opt.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication*	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Req.	Req.	Req.
Authorization	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Req.	Req.	Req.
Encryption**	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Opt.	Req.	Req.

Security Framework Template

Application to Application/ Server to Server												
Access	Opt.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication*	Opt.	Req.	Req.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.	Opt.
Authorization	Opt.	Req.	Req.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.	Opt.
Encryption**	Opt.	Opt.	Opt.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.	Opt.
Management Controls												
Asset Management	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Ad-Hoc	Req.	Req.
Configuration Management***	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
Physical Access Controls	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
Documented User Access / Certificate Policy & Process	Opt.	Opt.	Opt.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.	Opt.
Audit Controls												
Configuration Audit & Integrity Check	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Physical Access Audit	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc

Security Framework Template

Audited User Access / Certificate Policy & Process	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Data Access Audit	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Vulnerability Assessment	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Operational Controls												
Firewall/Access Control****	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
IDS/IPS - Network	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Opt.	TBD	Opt.	Opt.	Opt.
IDS/IPS - Host	Opt.	Opt.	Opt.	Req.	Req.	Req.	Req.	Opt.	TBD	Opt.	Opt.	Opt.

*** Authentication should be performed via encrypted channel when dealing with system administration or confidential data access.**

**** Encryption applies to data in transit**

***** Must follow Statewide Vulnerability Management Standard**

****** Must follow Statewide Firewall Standard**

******* Application Unique Domain To Be Determined (TBD) provides the ability for non-conforming applications to have a custom designed network security architecture that provides additional security measures as needed to mitigate identified risks.**

ISO 17799: 2005 REFERENCE
11.11.1 Access control policy

Office of the Governor
State Chief Information Officer

020116 Access Standard

Purpose: To establish a standard to limit access to business resources.

STANDARD

Agencies shall establish and enforce information security policies to limit access to State resources. Policies shall ensure that only authorized devices/persons have access as is appropriate for an agency in accordance with the agency's business needs.

Access policies shall be in accordance with *State Access Control Policies – 020101 to 020115.*

ISO 17799: 2005 REFERENCE
11.11.1 Access control policy

020117 Controlled Pathway

Purpose: To establish a standard to limit access to business resources.

STANDARD

A controlled pathway shall be used in Agency networks to assist in secure communications. Controlled paths shall be specified for remote users and local users when accessing business resources.

GUIDELINES

Special considerations should be given to limit roaming on wireless networks and restricting access to business applications through the use of zones listed in the Table set forth in Standard 020113.

ISO 17799: 2005 REFERENCE
11.4.2 User authentication for external connections

020118 Node Authentication

Purpose: To verify authentication processes are operating properly.

STANDARD

Procedures that verify node authentication measures shall be developed and tested on a semi-annual basis.

GUIDELINES

Testing should occur on the following connections to verify proper operational behavior:

- Remote user – VPN authentication.
- Dial back; dial backup and dial-up authentication mechanisms.
- Wireless authentication.
- Server authentication (email, domain logon, secure portals, etc.)

ISO 17799: 2005 REFERENCE
11.4.2 User authentication for external connections

020119 Diagnostic and Configuration Port Controls

Purpose: To control both physical and logical access to diagnostic and configuration ports.

STANDARD

Diagnostic and configuration ports shall be restricted to authorized individuals.

GUIDELINES

- Services that aren't required for business use should be disabled.
- Ports that aren't required for business use should be closed.

ISO 17799: 2005 REFERENCE
11.4.4 Remote diagnostic and configuration port protection

020120 Granting Access to Customers

Purpose: To ensure security arrangements are in place prior to granting customer or third party system access.

STANDARD

Customers and third parties must agree to adhere to all applicable Agency security policies and standards prior to receiving access to building facilities or information systems.

GUIDELINES

Safeguards to ensure customers agree to policies and standards should include:

- A written justification or purpose for access.
- Guest badges or alternate identification so staff may recognize the identity of the visiting person.
- Informational material to inform the accessing person(s) of responsibilities.

- A discrete notification of services authorized to access.
- A discrete disclaimer that system access may be monitored.

ISO 17799: 2005 REFERENCE
6.2.2 Addressing security when dealing with customers

020121 Acceptable Usage of Information Assets

Purpose: To ensure information assets are used in an acceptable fashion by customer or third parties.

STANDARD

Agencies shall develop Acceptable Use Policies (AUP's) or standards for staff, customers and third parties to follow.

GUIDELINES

AUP's and/or standards should focus at a minimum on the use of E-mail, Internet, and computing devices.

ISO 17799: 2005 REFERENCE
7.1.3 Acceptable use of assets

020122 Management Duties

Purpose: To use ensure management duties include compliance to information security policies and procedures.

STANDARD

All levels of management must ensure that employees, contractors, and third parties adhere to approved information security procedures.

Management duties shall include, but not be limited to ensuring staff:

- Become informed about security responsibilities.
- Attain continued education relevant to information security and their position in the organization.
- Are held contractually accountable for the proper use of those procedures, if applicable.
- Possess the necessary skills and qualifications to carry out their task(s) appropriately.
- Work to keep skills current within the technology

ISO 17799: 2005 REFERENCE
8.2.1 Management duties

020123 Third Party Service Management

Purpose: To use ensure management of Service level agreements with third parties.

STANDARD

Agencies shall manage third parties to meet or exceed mutually agreed upon signed service level agreements. Agencies shall also ensure that third parties meet or exceed all State policies, standards and procedures.

ISO 17799: 2005 REFERENCE
10.2.1 Service delivery

020124 Monitoring Third Party Services

Purpose: To monitor Service level agreements and invoke penalty clauses as appropriate.

STANDARD

Services, outputs and products provided by third parties shall be reviewed and checked regularly.

To monitor third party deliverables, Agencies shall:

- Monitor service performance of third party vendor to ensure service levels are up to contract requirements.
- Review reports provided by third parties and arrange regular meetings as required by service level agreement(s).
- Provide information concerning security incidents to the information security office.
- Review third party reports including the following, but not limited to, audit logs, operational problems, failures, fault analysis, as they relate to services being delivered, including security events.
- Resolve and manage any identified problem areas.

ISO 17799: 2005 REFERENCE
10.2.2 Monitoring and review of third party services

020125 Third Party Service Changes

Purpose: To ensure changes to services by third parties are agreed upon prior to the changes taking place.

STANDARD

Any changes to services being provided by a third party must be approved by the Agency head prior to implementation. Service level agreements need to be updated to reflect the changes that occur.

Examples to changes in service level agreements may include the following:

- Service improvements
- New or updated applications
- New controls
- Changes to network design
- New technologies, products or tools
- Changes in agency policies and procedures
- Resolve discovered exposures and changes that would improve the security posture of the agency.
- Change of vendors
- Services that are moved to a new or different location by the third party.

ISO 17799: 2005 REFERENCE
10.2.3 Managing changes to third party services

HISTORY

Approved by State CIO : November 18, 2005
Original Issue Date: November 18, 2005
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Information Asset Protection	010101 – Defining Information
	010103 – Storing and Handling Classified Information
	020121 – Acceptable Usage of Information Assets
Use of the State Network (Acceptable Use)	020121 – Acceptable Usage of Information Assets
	030303 – Sending Electronic Mail
	030312 – Using the Internet for Work Purposes
	100301 – Using the internet in an Acceptable Way
Identification and Authentication using IDS and Passwords	020106 – Managing Passwords
	050706 – Logon and Logoff from your Computer
	100302 – Keeping Passwords/PIN Numbers Confidential
User ID and Password Standard	020106 – Managing Passwords
	050403 – Using Laptop/Portable Computers

	100302 – Keeping Passwords/PIN Numbers Confidential
Desktop and Laptop Security Standard	020106- Managing Passwords
	030902 – Loading Personal Screensavers
	050402 – Issuing Laptop/Portable Computers to Personnel
	050403 – Using Laptop/Portable Computers
	050408 – Day-to-Day Use of Laptop/Portable Computers
	050705 – Clear Screen
	050706 – Logon and Logoff from your Computer
Security Framework Standard	020115 – Access Control Framework